CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
DEFEND TODAY, SECURE TOMORROW

Vulnerability Summary for the Week of May 31, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 06/07/2021 11:07 AM EDT

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
DEFEND TODAY, SECURE TOMORROW

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of May 31, 2021

06/07/2021 07:20 AM EDT

Original release date: June 7, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gnome -- gdk-pixbuf	A flaw was found in gdk-pixbuf in versions before 2.42.0. An integer wraparound leading to an out of bounds write can occur when a crafted GIF image is loaded. An attacker may cause applications to crash or could potentially execute code on the victim system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-28	8.3	CVE-2021-20240 MISC FEDORA FEDORA FEDORA
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 DQM API allows submitting of all control requests in unauthenticated sessions. This allows a remote attacker who can access a valid CA endpoint to read and write files to the Cognos Analytics system. IBM X-Force ID: 183903.	2021-06-01	7.5	CVE-2020-4561 CONFIRM XF
linux -- linux_kernel	There is a flaw reported in the Linux kernel in versions before 5.9 in drivers/gpu/drm/nouveau/nouveau_sgdma.c in nouveau_sgdma_create_ttm in Nouveau DRM subsystem. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker with a local account with a root privilege, can leverage this vulnerability to escalate privileges and execute code in the context of the kernel.	2021-05-28	7.2	CVE-2021-20292 MISC
linuxfoundation -- dex	A vulnerability exists in the SAML connector of the github.com/dexidp/dex library used to process SAML Signature Validation. This flaw allows an attacker to bypass SAML authentication. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. This flaw affects dex versions before 2.27.0.	2021-05-28	7.5	CVE-2020-27847 MISC MISC MISC
zeromq -- zeromq	A flaw was found in the ZeroMQ server in versions before 4.3.3. This flaw allows a malicious client to cause a stack buffer overflow on the server by sending crafted topic subscription requests and then unsubscribing. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-05-28	7.5	CVE-2021-20236 MISC MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cesanta -- mjs	Stack overflow vulnerability in parse_plus_minus Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36372 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cesanta -- mjs	Stack overflow vulnerability in parse_statement Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36368 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_value Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36366 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_comparison Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36374 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_array Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-18392 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_equality Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36375 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_shifts Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36373 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_statement_list Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36369 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_mul_div_rem Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36371 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_unary Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36370 MISC
cesanta -- mjs	Stack overflow vulnerability in parse_block Cesanta MJS 1.20.1, allows remote attackers to cause a Denial of Service (DoS) via a crafted file.	2021-05-28	4.3	CVE-2020-36367 MISC
css-what_project -- css-what	The css-what package before 5.0.1 for Node.js does not ensure that attribute parsing has Linear Time Complexity relative to the size of the input.	2021-05-28	5	CVE-2021-33587 MISC
gnu -- gama	A NULL-pointer deference issue was discovered in GNU_gama::set() in ellipsoid.h in Gama 2.04 which can lead to a denial of service (DOS) via segment faults caused by crafted inputs.	2021-05-28	5	CVE-2020-18395 MISC
ibm -- application_gateway	IBM Security Verify Access 20.07 could allow a remote attacker to send a specially crafted HTTP GET request that could cause the application to crash.	2021-06-01	5	CVE-2021-20576 XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain credentials from a user's browser via incorrect autocomplete settings in New Content Backup page. IBM X-Force ID: 172130.	2021-06-01	5	CVE-2019-4724 XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain credentials from a user's browser via incorrect autocomplete settings in New Data Server Connection page. IBM X-Force ID: 172129.	2021-06-01	5	CVE-2019-4723 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information, caused by the failure to set the secure flag for a sensitive cookie in an HTTPS session. A remote attacker could exploit this vulnerability to obtain sensitive information. IBM X-Force ID: 163780.	2021-06-01	4	CVE-2019-4471 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 172533.	2021-06-01	5.5	CVE-2019-4730 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to inject malicious HTML code that when viewed by the authenticated victim would execute the code. IBM X-Force ID: 182395.	2021-06-01	6.8	CVE-2020-4520 XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 176607.	2021-06-01	6.4	CVE-2020-4300 CONFIRM XF
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information via a stack trace due to mishandling of certain error conditions. IBM X-Force ID: 172128.	2021-06-01	4	CVE-2019-4722 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- security_verify_access	IBM Security Verify Access 20.07 could disclose sensitive information in HTTP server headers that could be used in further attacks against the system. IBM X-Force ID: 199398.	2021-06-01	5	CVE-2021-20585 XF CONFIRM
idreamsoft -- icms	A Cross Site Request Forgery (CSRF) vulnerability was discovered in iCMS 7.0.16 which can allow an attacker to execute arbitrary web scripts.	2021-05-28	6.8	CVE-2020-26641 MISC
kiali -- kiali	An authentication bypass vulnerability was found in Kiali in versions before 1.31.0 when the authentication strategy \`OpenID\` is used. When RBAC is enabled, Kiali assumes that some of the token validation is handled by the underlying cluster. When OpenID \`implicit flow\` is used with RBAC turned off, this token validation doesn't occur, and this allows a malicious user to bypass the authentication.	2021-05-28	5.8	CVE-2021-20278 MISC MISC
naver -- comic_viewer	An exposed remote debugging port in Naver Comic Viewer prior to 1.0.15.0 allowed a remote attacker to execute arbitrary code via a crafted HTML page.	2021-05-28	6.8	CVE-2021-33591 CONFIRM
openldap -- openldap	A flaw was found in OpenLDAP in versions before 2.4.56. This flaw allows an attacker who sends a malicious packet processed by OpenLDAP to force a failed assertion in csnNormalize23(). The highest threat from this vulnerability is to system availability.	2021-05-28	5	CVE-2020-25710 MLIST MISC DEBIAN MISC
redhat -- 389_directory_server	When using a sync_repl client in 389-ds-base, an authenticated attacker can cause a NULL pointer dereference using a specially crafted query, causing a crash.	2021-05-28	4	CVE-2021-3514 MISC
redhat -- keycloak	A flaw was found in keycloak in versions before 13.0.0. A Self Stored XSS attack vector escalating to a complete account takeover is possible due to user-supplied data fields not being properly encoded and Javascript code being used to process the data. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-05-28	6.8	CVE-2021-20195 MISC
redhat -- keycloak	A flaw was found in Keycloak before version 12.0.0 where it is possible to update the user's metadata attributes using Account REST API. This flaw allows an attacker to change its own NameID attribute to impersonate the admin user for any particular application.	2021-05-28	4.9	CVE-2020-27826 MISC
seacms -- seacms	A cross-site scripting (XSS) vulnerability has been discovered in the login page of SeaCMS version 11 which allows an attacker to inject arbitrary web script or HTML.	2021-05-28	4.3	CVE-2020-26642 MISC
spice_project -- spice	A flaw was found in spice in versions before 0.14.92. A DoS tool might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection.	2021-05-28	5	CVE-2021-20201 MISC MISC
trim-newlines_project -- trim-newlines	The trim-newlines package before 3.0.1 and 4.x before 4.0.1 for Node.js has an issue related to regular expression denial-of-service (ReDoS) for the .end() method.	2021-05-28	5	CVE-2021-33623 MISC CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 170964.	2021-06-01	3.5	CVE-2019-4653 XF CONFIRM
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178506.	2021-06-01	3.5	CVE-2020-4354 XF CONFIRM
linux -- linux_kernel	A flaw was found in the Linux kernel in versions before 5.4.92 in the BPF protocol. This flaw allows an attacker with a local account to leak information about kernel internal addresses. The highest threat from this vulnerability is to confidentiality.	2021-05-28	2.1	CVE-2021-20239 MISC
qemu -- qemu	A NULL pointer dereference flaw was found in the SCSI emulation support of QEMU in versions before 6.0.0. This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	2021-05-28	2.1	CVE-2020-35504 MLIST MISC MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1cdn -- 1cdn	1CDN is open-source file sharing software. In 1CDN before commit f88a2730fa50fc2c2aeab09011f6f142fd90ec25, there is a basic cross-site scripting vulnerability that allows an attacker to inject /<script>//code</script> and execute JavaScript code on the client side.	2021-05-28	not yet calculated	CVE-2021-32616 CONFIRM MISC
3scale -- developer	It was found that all versions of 3Scale developer portal lacked brute force protections. An attacker could use this gap to bypass login controls, and access privileged information, or possibly conduct further attacks.	2021-06-01	not yet calculated	CVE-2021-3412 MISC
aomedia -- libaom	aom_dsp/grain_table.c in libaom in AOMedia before 2021-03-30 has a use-after-free.	2021-06-02	not yet calculated	CVE-2021-30474 MISC MISC
aomedia -- libaom	aom_dsp/noise_model.c in libaom in AOMedia before 2021-03-24 has a buffer overflow.	2021-06-04	not yet calculated	CVE-2021-30475 MISC MISC
apache -- dubbo	In Apache Dubbo prior to 2.6.9 and 2.7.9, the usage of parseURL method will lead to the bypass of white host check which can cause open redirect or SSRF vulnerability.	2021-06-01	not yet calculated	CVE-2021-25640 MISC MLIST
apache -- dubbo	Apache Dubbo prior to 2.6.9 and 2.7.9 by default supports generic calls to arbitrary methods exposed by provider interfaces. These invocations are handled by the GenericFilter which will find the service and method specified in the first arguments of the invocation and use the Java Reflection API to make the final call. The signature for the $invoke or $invokeAsync methods is Ljava/lang/String;[Ljava/lang/String;[Ljava/lang/Object; where the first argument is the name of the method to invoke, the second one is an array with the parameter types for the method being invoked and the third one is an array with the actual call arguments. In addition, the caller also needs to set an RPC attachment specifying that the call is a generic call and how to decode the arguments. The possible values are: - true - raw.return - nativejava - bean - protobuf-json An attacker can control this RPC attachment and set it to nativejava to force the java deserialization of the byte array located in the third argument.	2021-06-01	not yet calculated	CVE-2021-30179 MLIST MISC
apache -- dubbo	Each Apache Dubbo server will set a serialization id to tell the clients which serialization protocol it is working on. But for Dubbo versions before 2.7.8 or 2.6.9, an attacker can choose which serialization id the Provider will use by tampering with the byte preamble flags, aka, not following the server's instruction. This means that if a weak deserializer such as the Kryo and FST are somehow in code scope (e.g. if Kryo is somehow a part of a dependency), a remote unauthenticated attacker can tell the Provider to use the weak deserializer, and then proceed to exploit it.	2021-06-01	not yet calculated	CVE-2021-25641 MISC
apache -- dubbo	Apache Dubbo prior to 2.7.9 support Tag routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these YAML rules, Dubbo customers may enable calling arbitrary constructors.	2021-06-01	not yet calculated	CVE-2021-30180 MISC
apache -- dubbo	Apache Dubbo prior to 2.6.9 and 2.7.9 supports Script routing which will enable a customer to route the request to the right server. These rules are used by the customers when making a request in order to find the right endpoint. When parsing these rules, Dubbo customers use ScriptEngine and run the rule provided by the script which by default may enable executing arbitrary code.	2021-06-01	not yet calculated	CVE-2021-30181 MISC
appcms -- appcms	AppCMS 2.0.101 in /admin/app.php has an arbitrary file deletion vulnerability which allows attackers to delete arbitrary files on the site.	2021-06-03	not yet calculated	CVE-2020-36005 MISC
appcms -- appcms	AppCMS 2.0.101 in /admin/template/tpl_app.php has a cross site scripting attack vulnerability which allows the attacker to obtain sensitive information of other users.	2021-06-03	not yet calculated	CVE-2020-36007 MISC
appcms -- appcms	AppCMS 2.0.101 in /admin/info.php has an arbitrary file deletion vulnerability which allows attackers to delete arbitrary files on the site.	2021-06-03	not yet calculated	CVE-2020-36006 MISC
appcms -- appcms	AppCMS 2.0.101 in /admin/download_frame.php has a SQL injection vulnerability which allows attackers to obtain sensitive database information.	2021-06-03	not yet calculated	CVE-2020-36004 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- multiple_products	Multiple buffer overflows in the (1) cdf_read_sat, (2) cdf_read_long_sector_chain, and (3) cdf_read_ssat function in file before 5.02.	2021-06-02	not yet calculated	CVE-2009-0948 MISC
apple -- multiple_products	Multiple integer overflows in the (1) cdf_read_property_info and (2) cdf_read_sat functions in file before 5.02.	2021-06-02	not yet calculated	CVE-2009-0947 MISC
auth0 -- auth0-lock	auth0-lock is Auth0's signin solution. Versions of nauth0-lock before and including `11.30.0` are vulnerable to reflected XSS. An attacker can execute arbitrary code when the library's `flashMessage` feature is utilized and user input or data from URL parameters is incorporated into the `flashMessage` or the library's `languageDictionary` feature is utilized and user input or data from URL parameters is incorporated into the `languageDictionary`. The vulnerability is patched in version 11.30.1.	2021-06-04	not yet calculated	CVE-2021-32641 MISC MISC CONFIRM
avahi -- avahi	A flaw was found in avahi in versions 0.6 up to 0.8. The event used to signal the termination of the client connection on the avahi Unix socket is not correctly handled in the client_work function, allowing a local attacker to trigger an infinite loop. The highest threat from this vulnerability is to the availability of the avahi service, which becomes unresponsive after this flaw is triggered.	2021-06-02	not yet calculated	CVE-2021-3468 MISC
backstage -- techdocs	Backstage is an open platform for building developer portals, and techdocs-common contains common functionalities for Backstage's TechDocs. In `@backstage/techdocs-common` versions prior to 0.6.3, a malicious actor could read sensitive files from the environment where TechDocs documentation is built and published by setting a particular path for `docs_dir` in `mkdocs.yml`. These files would then be available over the TechDocs backend API. This vulnerability is mitigated by the fact that an attacker would need access to modify the `mkdocs.yml` in the documentation source code, and would also need access to the TechDocs backend API. The vulnerability is patched in the `0.6.3` release of `@backstage/techdocs-common`.	2021-06-03	not yet calculated	CVE-2021-32662 MISC MISC CONFIRM
backstage -- techdocs	Backstage is an open platform for building developer portals, and techdocs-common contains common functionalities for Backstage's TechDocs. In versions of `@backstage/tehdocs-common` prior to 0.6.4, a malicious internal actor is able to upload documentation content with malicious scripts. These scripts would normally be sanitized by the TechDocs frontend, but by tricking a user to visit the content via the TechDocs API, the content sanitazion will be bypassed. If the TechDocs API is hosted on the same origin as the Backstage app or other backend plugins, this may give access to sensitive data. The ability to upload malicious content may be limited by internal code review processes, unless the chosen TechDocs deployment method is to use an object store and the actor has access to upload files directly to that store. The vulnerability is patched in the `0.6.4` release of `@backstage/techdocs-common`.	2021-06-03	not yet calculated	CVE-2021-32660 CONFIRM MISC MISC
backstage -- techdocs	Backstage is an open platform for building developer portals. In versions of Backstage's Techdocs Plugin (`@backstage/plugin-techdocs`) prior to 0.9.5, a malicious internal actor can potentially upload documentation content with malicious scripts by embedding the script within an `object` element. This may give access to sensitive data when other users visit that same documentation page. The ability to upload malicious content may be limited by internal code review processes, unless the chosen TechDocs deployment method is to use an object store and the actor has access to upload files directly to that store. The vulnerability is patched in the `0.9.5` release of `@backstage/plugin-techdocs`.	2021-06-03	not yet calculated	CVE-2021-32661 CONFIRM MISC MISC
bdew -- bdlib	The BDew BdLib library before 1.16.1.7 for Minecraft allows remote code execution because it deserializes untrusted data in ObjectInputStream.readObject as part of its use of Java serialization.	2021-06-03	not yet calculated	CVE-2021-33806 MISC CONFIRM MISC MISC
bigtree_cms -- bigtree_cms	A SQL injection vulnerability was discovered in /core/feeds/custom.php in BigTree CMS 4.4.10 and earlier which allows an authenticated attacker to inject a malicious SQL query to the applications via the 'Create New Feed' function.	2021-06-01	not yet calculated	CVE-2020-26668 MISC
bigtree_cms -- bigtree_cms	A vulnerability has been discovered in BigTree CMS 4.4.10 and earlier which allows an authenticated attacker to execute arbitrary commands through a crafted request sent to the server via the 'Create a New Setting' function.	2021-06-01	not yet calculated	CVE-2020-26670 MISC
bigtree_cms -- bigtree_cms	A stored cross-site scripting (XSS) vulnerability was discovered in BigTree CMS 4.4.10 and earlier which allows an authenticated attacker to execute arbitrary web scripts or HTML via the page content to site/index.php/admin/pages/update.	2021-06-01	not yet calculated	CVE-2020-26669 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bird -- bird	** DISPUTED ** BIRD through 2.0.7 does not provide functionality for password authentication of BGP peers. Because of this, products that use BIRD (which may, for example, include Tigera products in some configurations, as well as products of other vendors) may have been susceptible to route redirection for Denial of Service and/or Information Disclosure. NOTE: a researcher has asserted that the behavior is within Tigera's area of responsibility; however, Tigera disagrees.	2021-06-04	not yet calculated	CVE-2021-26928 MISC
bloofoxcms -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Unrestricted File Upload vulnerability via bypass MIME Type validation by inserting 'image/jpeg' within the 'Content-Type' header.	2021-06-04	not yet calculated	CVE-2020-36141 MISC
bloofoxcms -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Directory traversal vulnerability by inserting '../' payloads within the 'fileurl' parameter.	2021-06-04	not yet calculated	CVE-2020-36142 MISC
bloofoxcms -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Cross-Site Request Forgery (CSRF) via 'mode=settings&page=editor', as demonstrated by use of 'mode=settings&page=editor' to change any file content (Locally/Remotely).	2021-06-04	not yet calculated	CVE-2020-36140 MISC
bloofoxcms -- bloofoxcms	BloofoxCMS 0.5.2.1 allows Reflected Cross-Site Scripting (XSS) vulnerability by inserting a XSS payload within the 'fileurl' parameter.	2021-06-04	not yet calculated	CVE-2020-36139 MISC
bpmn -- editor	A flaw was found in the BPMN editor in version jBPM 7.51.0.Final. Any authenticated user from any project can see the name of Ruleflow Groups from other projects, despite the user not having access to those projects. The highest threat from this vulnerability is to confidentiality.	2021-06-01	not yet calculated	CVE-2021-20306 MISC
bubble_fireworks -- bubble_fireworks	bubble fireworks is an open source java package relating to Spring Framework. In bubble fireworks before version 2021.BUILD-SNAPSHOT there is a vulnerability in which the package did not properly verify the signature of JSON Web Tokens. This allows to forgery of valid JWTs.	2021-06-04	not yet calculated	CVE-2021-29500 CONFIRM
chiyu_technology -- multiple_iot_devices	Multiple storage XSS vulnerabilities were discovered on BF-430, BF-431 and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of sanitization of the input on the components man.cgi, if.cgi, dhcpc.cgi, ppp.cgi.	2021-06-04	not yet calculated	CVE-2021-31250 MISC MISC MISC
chiyu_technology -- multiple_iot_devices	A CRLF injection vulnerability was found on BF-430, BF-431, and BF-450M TCP/IP Converter devices from CHIYU Technology Inc due to a lack of validation on the parameter redirect= available on multiple CGI components.	2021-06-04	not yet calculated	CVE-2021-31249 MISC MISC MISC
chiyu_technology -- multiple_iot_devices	An open redirect vulnerability exists in BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, and SEMAC devices from CHIYU Technology that can be exploited by sending a link that has a specially crafted URL to convince the user to click on it.	2021-06-04	not yet calculated	CVE-2021-31252 CONFIRM MISC MISC
chiyu_technology -- multiple_iot_devices	An unauthenticated XSS vulnerability exists in several IoT devices from CHIYU Technology, including BF-630, BF-450M, BF-430, BF-431, BF631-W, BF830-W, Webpass, BF-MINI-W, and SEMAC due to a lack of sanitization when the HTTP 404 message is generated.	2021-06-01	not yet calculated	CVE-2021-31641 MISC MISC MISC MISC
chiyu_technology -- multiple_iot_devices	An authentication bypass in telnet server in BF-430 and BF431 232/422 TCP/IP Converter, BF-450M and SEMAC from CHIYU Technology Inc allows obtaining a privileged connection with the target device by supplying a specially malformed request and an attacker may force the remote telnet server to believe that the user has already authenticated.	2021-06-04	not yet calculated	CVE-2021-31251 CONFIRM MISC MISC
chiyu_technology -- multiple_iot_devices	An XSS vulnerability exists in several IoT devices from CHIYU Technology, including SEMAC, Biosense, BF-630, BF-631, and Webpass due to a lack of sanitization on the component if.cgi - username parameter.	2021-06-01	not yet calculated	CVE-2021-31643 MISC MISC MISC MISC
chiyu_technology -- multiple_iot_devices	A denial of service condition exists after an integer overflow in several IoT devices from CHIYU Technology, including BIOSENSE, Webpass, and BF-630, BF-631, and SEMAC. The vulnerability can be explored by sending an unexpected integer (> 32 bits) on the page parameter that will crash the web portal and making it unavailable until a reboot of the device.	2021-06-01	not yet calculated	CVE-2021-31642 MISC MISC MISC MISC
cisco -- asr_5000_series_software	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2021-06-04	not yet calculated	CVE-2021-1540 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- asr_5000_series_software	Multiple vulnerabilities in the authorization process of Cisco ASR 5000 Series Software (StarOS) could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2021-06-04	not yet calculated	CVE-2021-1539 CISCO
cisco -- common_services_platform_collecto	A vulnerability in the configuration dashboard of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to execute arbitrary code. This vulnerability is due to insufficient sanitization of configuration entries. An attacker could exploit this vulnerability by logging in as a super admin and entering crafted input to configuration options on the CSPC configuration dashboard. A successful exploit could allow the attacker to execute remote code as root.	2021-06-04	not yet calculated	CVE-2021-1538 CISCO
cisco -- ds-wan_software	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. This vulnerability exists because the affected software does not properly restrict access to privileged processes. An attacker could exploit this vulnerability by invoking a privileged process in the affected system. A successful exploit could allow the attacker to perform actions with the privileges of the root user.	2021-06-04	not yet calculated	CVE-2021-1528 CISCO
cisco -- multiple_products	A vulnerability in Cisco Webex Meetings Desktop App for Windows, Cisco Webex Meetings Server, Cisco Webex Network Recording Player for Windows, and Cisco Webex Teams for Windows could allow an authenticated, local attacker to perform a DLL injection attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. This vulnerability is due to incorrect handling of directory paths at run time. An attacker could exploit this vulnerability by inserting a configuration file in a specific path in the system, which can cause a malicious DLL file to be loaded when the application starts. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of another user account.	2021-06-04	not yet calculated	CVE-2021-1536 CISCO
cisco -- thousandeyes_recorder	A vulnerability in the installer software of Cisco ThousandEyes Recorder could allow an unauthenticated, local attacker to access sensitive information that is contained in the ThousandEyes Recorder installer software. This vulnerability exists because sensitive information is included in the application installer. An attacker could exploit this vulnerability by downloading the installer and extracting its contents. A successful exploit could allow the attacker to access sensitive information that is included in the application installer.	2021-06-04	not yet calculated	CVE-2021-1537 CISCO
cisco -- video_surveillance_7000_series_ip+cameras	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery Protocol or LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2021-06-04	not yet calculated	CVE-2021-1564 CISCO
cisco -- video_surveillance_7000_series_ip_cameras	Multiple vulnerabilities in the implementation of the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain Cisco Discovery Protocol and LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted Cisco Discovery Protocol or LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: Cisco Discovery Protocol and LLDP are Layer 2 protocols. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2021-06-04	not yet calculated	CVE-2021-1563 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- webex_meetings	A vulnerability in logging mechanisms of Cisco Webex Meetings client software could allow an authenticated, local attacker to gain access to sensitive information. This vulnerability is due to unsafe logging of application actions. An attacker could exploit this vulnerability by logging onto the local system and accessing files containing the logged details. A successful exploit could allow the attacker to gain access to sensitive information, including meeting data and recorded meeting transcriptions.	2021-06-04	not yet calculated	CVE-2021-1544 CISCO
cisco -- webex_meetings_and_meeterings_server	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to redirect users to a malicious file. This vulnerability is due to improper validation of URL paths in the application interface. An attacker could exploit this vulnerability by persuading a user to follow a specially crafted URL that is designed to cause Cisco Webex Meetings to include a remote file in the web UI. A successful exploit could allow the attacker to cause the application to offer a remote file to a user, which could allow the attacker to conduct further phishing or spoofing attacks.	2021-06-04	not yet calculated	CVE-2021-1525 CISCO
cisco -- webex_meetings_and_meetings_server	A vulnerability in the multimedia viewer feature of Cisco Webex Meetings and Cisco Webex Meetings Server could allow an authenticated, remote attacker to bypass security protections. This vulnerability is due to unsafe handling of shared content within the multimedia viewer feature. An attacker could exploit this vulnerability by sharing a file through the multimedia viewer feature. A successful exploit could allow the attacker to bypass security protections and prevent warning dialogs from appearing before files are offered to other users.	2021-06-04	not yet calculated	CVE-2021-1517 CISCO
cisco -- webex_network_recording_player	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. The vulnerability is due to insufficient validation of values within Webex recording files formatted as either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit the vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	2021-06-04	not yet calculated	CVE-2021-1502 CISCO
cisco -- webex_network_recording_player	A vulnerability in Cisco Webex Network Recording Player for Windows and MacOS and Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. This vulnerability is due to insufficient validation of values in Webex recording files that are in either Advanced Recording Format (ARF) or Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	2021-06-04	not yet calculated	CVE-2021-1503 CISCO
cisco -- webex_player	A vulnerability in Cisco Webex Player for Windows and MacOS could allow an attacker to execute arbitrary code on an affected system. This vulnerability is due to insufficient validation of values in Webex recording files that are in Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the targeted user.	2021-06-04	not yet calculated	CVE-2021-1526 CISCO
cisco -- webex_player	A vulnerability in Cisco Webex Player for Windows and MacOS could allow an attacker to cause the affected software to terminate or to gain access to memory state information that is related to the vulnerable application. The vulnerability is due to insufficient validation of values in Webex recording files that are stored in Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a malicious WRF file to a user as a link or email attachment and then persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to crash the affected software and view memory state information.	2021-06-04	not yet calculated	CVE-2021-1527 CISCO
clustered_data -- ontap	Clustered Data ONTAP versions prior to 9.7P13 and 9.8P3 are susceptible to a vulnerability which could allow single workloads to cause a Denial of Service (DoS) on a cluster node.	2021-06-04	not yet calculated	CVE-2021-26994 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cms_made_simple -- cms_made_simple	A cross-site scripting (XSS) vulnerability was discovered in the Administrator panel on the 'Setting News' module on CMS Made Simple 2.2.14 which allows an attacker to execute arbitrary web scripts.	2021-06-01	not yet calculated	CVE-2020-27377 MISC
d-link -- dir-868l_router	The D-Link router DIR-868L 3.01 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	2021-06-04	not yet calculated	CVE-2020-29321 MISC
d-link -- dir-880l_router	The D-Link router DIR-880L 1.07 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	2021-06-04	not yet calculated	CVE-2020-29322 MISC
d-link -- dir-885l-mfc_router	The D-link router DIR-885L-MFC 1.15b02, v1.21b05 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	2021-06-04	not yet calculated	CVE-2020-29323 MISC
d-link -- dir-895l-mfc_router	The DLink Router DIR-895L MFC v1.21b05 is vulnerable to credentials disclosure in telnet service through decompilation of firmware, that allows an unauthenticated attacker to gain access to the firmware and to extract sensitive data.	2021-06-04	not yet calculated	CVE-2020-29324 MISC
debian -- debian	The open_generic_xdg_mime function in xdg-open in xdg-utils 1.1.0 rc1 in Debian, when using dash, does not properly handle local variables, which allows remote attackers to execute arbitrary commands via a crafted file.	2021-06-02	not yet calculated	CVE-2015-1877 MISC MISC MISC MISC MISC MISC
eclipse -- moiarra	Directory traversal in Eclipse Mojarra before 2.3.14 allows attackers to read arbitrary files via the loc parameter or con parameter.	2021-06-02	not yet calculated	CVE-2020-6950 MISC MISC MISC
emissary -- emissary	Emissary is a P2P based data-driven workflow engine. Affected versions of Emissary are vulnerable to post-authentication Remote Code Execution (RCE). The [`CreatePlace`](https://github.com/NationalSecurityAgency/emissary/blob/30c54ef16c6eb6ed09604a929939fb9f66868382/src/main/ja REST endpoint accepts an `sppClassName` parameter which is used to load an arbitrary class. This class is later instantiated using a constructor with the following signature: `<constructor>(String, String, String)`. An attacker may find a gadget (class) in the application classpath that could be used to achieve Remote Code Execution (RCE) or disrupt the application. Even though the chances to find a gadget (class) that allow arbitrary code execution are low, an attacker can still find gadgets that could potentially crash the application or leak sensitive data. As a work around disable network access to Emissary from untrusted sources.	2021-06-01	not yet calculated	CVE-2021-32647 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
envoy -- envoy	### Description Envoy does not decode escaped slash sequences `%2F` and `%5C` in HTTP URL paths in versions 1.18.2 and before. A remote attacker may craft a path with escaped slashes, e.g. `/something%2F..%2Fadmin`, to bypass access control, e.g. a block on `/admin`. A backend server could then decode slash sequences and normalize path and provide an attacker access beyond the scope provided for by the access control policy. ### Impact Escalation of Privileges when using RBAC or JWT filters with enforcement based on URL path. Users with back end servers that interpret `%2F` and `/` and `%5C` and ` You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available. interchangeably are impacted. ### Attack Vector URL paths containing escaped slash characters delivered by untrusted client. ### Patches Envoy versions 1.18.3, 1.17.3, 1.16.4, 1.15.5 contain new path normalization option to decode escaped slash characters. ### Workarounds If back end servers treat `%2F` and `/` and `%5C` and ` You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available. interchangeably and a URL path based access control is configured, we recommend reconfiguring back end server to not treat `%2F` and `/` and `%5C` and ` You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available. interchangeably if feasible. ### Credit Ruilin Yang (ruilin.yrl@gmail.com) ### References https://blog.envoyproxy.io https://github.com/envoyproxy/envoy/releases ### For more information If you have any questions or comments about this advisory: * Open an issue in [Envoy repo](https://github.com/envoyproxy/envoy/issues) * Email us at [envoy-security](mailto:envoy-security@googlegroups.com)	2021-05-28	not yet calculated	CVE-2021-29492 CONFIRM
fdcms -- fdcms	FDCMS (also known as Fangfa Content Management System) 4.0 allows remote attackers to get a webshell in the background via Front/lib/Action/FindexAction.class.php.	2021-06-02	not yet calculated	CVE-2020-35442 MISC
fdcms -- fdcms	FDCMS (aka Fangfa Content Management System) 4.0 contains a front-end SQL injection via Admin/Lib/Action/FloginAction.class.php.	2021-06-02	not yet calculated	CVE-2020-35441 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the filter_frame function in vf_tile.c.	2021-06-02	not yet calculated	CVE-2020-22051 MISC MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in avcodec_alloc_context3 at options.c.	2021-06-01	not yet calculated	CVE-2020-22037 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the ff_v4l2_m2m_create_context function in v4l2_m2m.c.	2021-06-01	not yet calculated	CVE-2020-22038 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 idue to a memory leak in the v_frame_alloc function in frame.c.	2021-06-01	not yet calculated	CVE-2020-22040 MISC
ffmpeg -- ffmpeg	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 in filter_intra at libavfilter/vf_bwdif.c, which might lead to memory corruption and other potential consequences.	2021-06-01	not yet calculated	CVE-2020-22036 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the inavi_add_ientry function.	2021-06-01	not yet calculated	CVE-2020-22039 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak is affected by: memory leak in the link_filter_inouts function in libavfilter/graphparser.c.	2021-06-01	not yet calculated	CVE-2020-22042 MISC
ffmpeg -- ffmpeg	A heap-based Buffer Overflow vulnerability exists in FFmpeg 4.2 in get_block_row at libavfilter/vf_bm3d.c, which might lead to memory corruption and other potential consequences.	2021-06-01	not yet calculated	CVE-2020-22035 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the av_buffersrc_add_frame_flags function in buffersrc.	2021-06-01	not yet calculated	CVE-2020-22041 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the ff_frame_pool_get function in framepool.c.	2021-06-02	not yet calculated	CVE-2020-22048 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak at the fifo_alloc_common function in libavutil/fifo.c.	2021-06-01	not yet calculated	CVE-2020-22043 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the url_open_dyn_buf_internal function in libavformat/aviobuf.c.	2021-06-01	not yet calculated	CVE-2020-22044 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the avpriv_float_dsp_allocl function in libavutil/float_dsp.c.	2021-06-02	not yet calculated	CVE-2020-22046 MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the wtvfile_open_sector function in wtvdec.c.	2021-06-02	not yet calculated	CVE-2020-22049 MISC MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the av_dict_set function in dict.c.	2021-06-02	not yet calculated	CVE-2020-22054 MISC MISC
ffmpeg -- ffmpeg	A Denial of Service vulnerability exists in FFmpeg 4.2 due to a memory leak in the config_input function in af_acrossover.c.	2021-06-02	not yet calculated	CVE-2020-22056 MISC
foreman -- forman	Foreman versions before 2.3.4 and before 2.4.0 is affected by an improper authorization handling flaw. An authenticated attacker can impersonate the foreman-proxy if product enable the Puppet Certificate authority (CA) to sign certificate requests that have subject alternative names (SANs). Foreman do not enable SANs by default and `allow-authorization-extensions` is set to `false` unless user change `/etc/puppetlabs/puppetserver/conf.d/ca.conf` configuration explicitly.	2021-06-03	not yet calculated	CVE-2021-3469 MISC
fortinet -- forti_presence	Two authorization bypass through user-controlled key vulnerabilities in the Fortinet FortiPresence 2.1.0 administration interface may allow an attacker to gain access to some user data via portal manager or portal users parameters.	2021-06-02	not yet calculated	CVE-2020-6641 CONFIRM
fortinet -- fortiai	An improper input validation in FortiAI v1.4.0 and earlier may allow an authenticated user to gain system shell access via a malicious payload in the "diagnose" command.	2021-06-03	not yet calculated	CVE-2021-24023 CONFIRM
fortinet -- fortigate	An improper following of a certificate's chain of trust vulnerability in FortiGate versions 6.4.0 to 6.4.4 may allow an LDAP user to connect to SSLVPN with any certificate that is signed by a trusted Certificate Authority.	2021-06-02	not yet calculated	CVE-2021-24012 CONFIRM
fortinet -- fortiproxy	A stack-based buffer overflow vulnerability in FortiProxy physical appliance CLI 2.0.0 to 2.0.1, 1.2.0 to 1.2.9, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7 may allow an authenticated, remote attacker to perform a Denial of Service attack by running the `diagnose sys cpuset` with a large cpuset mask value. Fortinet is not aware of any successful exploitation of this vulnerability that would lead to code execution.	2021-06-03	not yet calculated	CVE-2021-22130 CONFIRM
fortinet -- fortiswitch	A missing release of memory after effective lifetime vulnerability in FortiSwitch 6.4.0 to 6.4.6, 6.2.0 to 6.2.6, 6.0.0 to 6.0.6, 3.6.11 and below may allow an attacker on an adjacent network to exhaust available memory by sending specifically crafted LLDP/CDP/EDP packets to the device.	2021-06-01	not yet calculated	CVE-2021-26111 CONFIRM
fortinet -- fortiweb	An OS command injection vulnerability in FortiWeb's management interface 6.3.7 and below, 6.2.3 and below, 6.1.x, 6.0.x, 5.9.x may allow a remote authenticated attacker to execute arbitrary commands on the system via the SAML server configuration page.	2021-06-01	not yet calculated	CVE-2021-22123 CONFIRM
freebsd -- freebsd	In FreeBSD 12.2-STABLE before r367402, 11.4-STABLE before r368202, 12.2-RELEASE before p1, 12.1-RELEASE before p11 and 11.4-RELEASE before p5 the handler for a routing option caches a pointer into the packet buffer holding the ICMPv6 message. However, when processing subsequent options the packet buffer may be freed, rendering the cached pointer invalid. The network stack may later dereference the pointer, potentially triggering a use-after-free.	2021-06-04	not yet calculated	CVE-2020-7469 MISC
frontier -- ichris	Frontier ichris through 5.18 allows users to upload malicious executable files that might later be downloaded and run by any client user.	2021-05-29	not yet calculated	CVE-2021-31703 MISC
frontier -- ichris	Frontier ichris through 5.18 mishandles making a DNS request for the hostname in the HTTP Host header, as demonstrated by submitting 127.0.0.1 multiple times for DoS.	2021-05-29	not yet calculated	CVE-2021-31702 MISC
fuse -- fuse	In the reference implementation of FUSE before 2.9.8 and 3.x before 3.2.5, local attackers were able to specify the allow_other option even if forbidden in /etc/fuse.conf, leading to exposure of FUSE filesystems to other users. This issue only affects systems with SELinux active.	2021-06-03	not yet calculated	CVE-2021-33805 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
genivi -- diagnostic_log_and_trace	GENIVI Diagnostic Log and Trace (DLT) provides a log and trace interface. In versions of GENIVI DLT between 2.10.0 and 2.18.6, a configuration file containing the special characters could cause a vulnerable component to crash. All the applications which are using the configuration file could fail to generate their dlt logs in system. As of time of publication, no patch exists. As a workaround, one may check the integrity of information in configuration file manually.	2021-05-28	not yet calculated	CVE-2021-29507 CONFIRM
github -- satori	A flaw was found in github.com/satori/go.uuid in versions from commit 0ef6afb2f6cdd6cdaeee3885a95099c63f18fc8c to d91630c8510268e75203009fe7daf2b8e1d60c45. Due to insecure randomness in the g.rand.Read function the generated UUIDs are predictable for an attacker.	2021-06-02	not yet calculated	CVE-2021-3538 MISC MISC MISC
glob-parent -- glob-parent	This affects the package glob-parent before 5.1.2. The enclosure regex used to check for strings ending in enclosure containing path separator.	2021-06-03	not yet calculated	CVE-2020-28469 MISC MISC MISC MISC MISC MISC
gnu -- libiberty	A flaw was discovered in GNU libiberty within demangle_path() in rust-demangle.c, as distributed in GNU Binutils version 2.36. A crafted symbol can cause stack memory to be exhausted leading to a crash.	2021-06-02	not yet calculated	CVE-2021-3530 MISC
google -- chrome	Use after free in File API in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30515 MISC MISC
google -- chrome	Heap buffer overflow in History in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30516 MISC MISC
google -- chrome	Heap buffer overflow in Media Feeds in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to enable certain features in Chrome to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30508 MISC MISC
google -- chrome	Inappropriate implementation in Offline in Google Chrome on Android prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30507 MISC MISC
google -- chrome	Incorrect security UI in Web App Installs in Google Chrome on Android prior to 90.0.4430.212 allowed an attacker who convinced a user to install a web application to inject scripts or HTML into a privileged page via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30506 MISC MISC
google -- chrome	Out of bounds read in Tab Groups in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30511 MISC MISC
google -- chrome	Use after free in Notifications in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30512 MISC MISC
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30513 MISC MISC
google -- chrome	Use after free in Autofill in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30514 MISC MISC
google -- chrome	Out of bounds write in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page and a crafted Chrome extension.	2021-06-04	not yet calculated	CVE-2021-30509 MISC MISC
google -- chrome	Use after free in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30520 MISC MISC
google -- chrome	Use after free in Aura in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30510 MISC MISC
google -- chrome	Use after free in Payments in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious payments app to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30519 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30517 MISC MISC
google -- chrome	Heap buffer overflow in Reader Mode in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-06-04	not yet calculated	CVE-2021-30518 MISC MISC
gstreamer -- gstreamer	GStreamer before 1.18.4 may perform an out-of-bounds read when handling certain ID3v2 tags.	2021-06-02	not yet calculated	CVE-2021-3522 MISC
hashicorp -- vault_and_vault_enterprise	HashiCorp Vault and Vault Enterprise allowed the renewal of nearly-expired token leases and dynamic secret leases (specifically, those within 1 second of their maximum TTL), which caused them to be incorrectly treated as non-expiring during subsequent use. Fixed in 1.5.9, 1.6.5, and 1.7.2.	2021-06-03	not yet calculated	CVE-2021-32923 MISC MISC
huawei -- smartphone	There is an Improper Access Control vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause app redirections.	2021-06-03	not yet calculated	CVE-2021-22334 MISC
huawei -- smartphone	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Attackers with physical access to the device can thereby exploit this vulnerability. A successful exploitation of this vulnerability can compromise the device's data security and functional availability.	2021-06-03	not yet calculated	CVE-2021-22316 MISC
huawei -- smartphone	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	2021-06-03	not yet calculated	CVE-2021-22317 MISC
huawei -- smartphone	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause leaking of user click data.	2021-06-03	not yet calculated	CVE-2021-22337 MISC
huawei -- smartphone	There is an Information Disclosure vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may result in video streams being intercepted during transmission.	2021-06-03	not yet calculated	CVE-2021-22325 MISC
huawei -- smartphone	There is a Business Logic Errors vulnerability in Huawei Smartphone. The malicious apps installed on the device can keep taking screenshots in the background. This issue does not cause system errors, but may cause personal information leakage.	2021-06-03	not yet calculated	CVE-2021-22308 MISC
huawei -- smartphone	There is an Improper Control of Generation of Code vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause denial of security services on a rooted device.	2021-06-03	not yet calculated	CVE-2021-22336 MISC
huawei -- smartphone	There is a Memory Buffer Improper Operation Limit vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause exceptions in image processing.	2021-06-03	not yet calculated	CVE-2021-22335 MISC
huawei -- smartphone	There is a Security Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	2021-06-03	not yet calculated	CVE-2021-22313 MISC
huawei -- smartphone	There is a Credentials Management Errors vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	2021-06-03	not yet calculated	CVE-2021-22324 MISC
huawei -- smartphone	There is a Missing Authentication for Critical Function vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may impair data confidentiality.	2021-06-03	not yet calculated	CVE-2021-22322 MISC
huawei -- smartphone	There is an Improper Validation of Array Index vulnerability in Huawei Smartphone. Successful exploitation of this vulnerability may cause code to execute, thus obtaining system permissions.	2021-06-03	not yet calculated	CVE-2021-22333 MISC
ibm -- engineering_lifestyle_optimization_publishing	IBM Engineering Lifecycle Optimization - Publishing is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 192470.	2021-06-02	not yet calculated	CVE-2020-4977 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-ForceID: 194597.	2021-06-02	not yet calculated	CVE-2021-20348 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 194449.	2021-06-02	not yet calculated	CVE-2021-20338 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products could allow an authenticated user to obtain sensitive information due to lack of security restrictions. IBM X-Force ID: 188126.	2021-06-02	not yet calculated	CVE-2020-4732 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199406.	2021-06-02	not yet calculated	CVE-2021-29668 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199408.	2021-06-02	not yet calculated	CVE-2021-29670 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to bypass security restrictions, caused by improper access control. By sending a specially-crafted request to the REST API, an attacker could exploit this vulnerability to bypass access restrictions, and execute arbitrary actions with administrative privileges. IBM X-Force ID: 182114.	2021-06-02	not yet calculated	CVE-2020-4495 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 193737.	2021-06-02	not yet calculated	CVE-2020-5030 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products could allow a remote attacker to obtain sensitive information when an error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 195516.	2021-06-02	not yet calculated	CVE-2021-20371 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194593.	2021-06-02	not yet calculated	CVE-2021-20343 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194595.	2021-06-02	not yet calculated	CVE-2021-20346 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194596.	2021-06-02	not yet calculated	CVE-2021-20347 CONFIRM XF
ibm -- jazz_foundation	IBM Jazz Foundation and IBM Engineering products are vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 194594.	2021-06-02	not yet calculated	CVE-2021-20345 CONFIRM XF
ibm -- qradar_advisor	IBM QRadar Advisor With Watson App 1.1 through 2.5 as used on IBM QRadar SIEM 7.4 could allow a remote user to obtain sensitive information from HTTP requests that could aid in further attacks against the system. IBM X-Force ID: 195712.	2021-06-03	not yet calculated	CVE-2021-20380 XF CONFIRM
ibm -- security_verify_access	IBM Security Verify Access 20.07 allows web pages to be stored locally which can be read by another user on the system. X-Force ID: 199278.	2021-06-01	not yet calculated	CVE-2021-20575 XF CONFIRM
ibm -- security_verify_access	IBM Security Verify Access 20.07 is vulnerable to a stack based buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with elevated privileges.	2021-06-01	not yet calculated	CVE-2021-29665 XF CONFIRM
ibm -- spectrum_scale	IBM Spectrum Scale 5.0.0 through 5.0.5.6 and 5.1.0 through 5.1.0.3 system core component is affected by a format string security vulnerability. An attacker could execute arbitrary code in the context of process memory, potentially escalating their system privileges and taking control over the entire system with root access. IBM X-Force ID: 201474.	2021-06-01	not yet calculated	CVE-2021-29740 CONFIRM XF
in4suite -- erp	SQL injection in In4Suite ERP 3.2.74.1370 allows attackers to modify or delete data, causing persistent changes to the application's content or behavior by using malicious SQL queries.	2021-06-01	not yet calculated	CVE-2021-27828 MISC MISC
infinispan -- infinispan	A flaw was found in Infinispan version 10, where it is possible to perform various actions that could have side effects using GET requests. This flaw allows an attacker to perform a cross-site request forgery (CSRF) attack.	2021-06-02	not yet calculated	CVE-2020-10771 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
invision_community -- invision_community	Invision Community (aka IPS Community Suite) before 4.6.0 allows eval-based PHP code injection by a moderator because the IPS\cms\modules\front\pages_builder::previewBlock method interacts unsafely with the IPS_Theme::runProcessFunction method.	2021-06-01	not yet calculated	CVE-2021-32924 MISC FULLDISC MISC MISC MISC
irzsz -- irzsz	lrzsz before version 0.12.21~rc can leak information to the receiving side due to an incorrect length check in the function zsdata that causes a size_t to wrap around.	2021-06-02	not yet calculated	CVE-2018-10195 MISC MISC MISC MISC
istio -- istio	Istio before 1.8.6 and 1.9.x before 1.9.5, when a gateway is using the AUTO_PASSTHROUGH routing configuration, allows attackers to bypass authorization checks and access unexpected services in the cluster.	2021-06-02	not yet calculated	CVE-2021-31921 MISC
jboss -- enterprise_application_platform	It was found that the issue for security flaw CVE-2019-3805 appeared again in a further version of JBoss Enterprise Application Platform - Continuous Delivery (EAP-CD) introducing regression. An attacker could exploit this by modifying the PID file in /var/run/jboss-eap/ allowing the init.d script to terminate any process as root.	2021-06-02	not yet calculated	CVE-2020-14317 MISC
jboss-remoting -- jboss-remoting	A flaw was found in jboss-remoting in versions before 5.0.20.SP1-redhat-00001. A malicious attacker could cause threads to hold up forever in the EJB server by writing a sequence of bytes corresponding to the expected messages of a successful EJB client request, but omitting the ACK messages, or just tamper with jboss-remoting code, deleting the lines that send the ACK message from the EJB client code resulting in a denial of service. The highest threat from this vulnerability is to system availability.	2021-06-02	not yet calculated	CVE-2020-35510 MISC
johnson_controls -- metasys	Successful exploitation of this vulnerability could give an authenticated Metasys user an unintended level of access to the server file system, allowing them to access or modify system files by sending specifically crafted web messages to the Metasys system. This issue affects: Johnson Controls Metasys version 11.0 and prior versions.	2021-06-04	not yet calculated	CVE-2021-27657 CERT CONFIRM
json -- smart	A vulnerability was discovered in the indexOf function of JSONParserByteArray in JSON Smart versions 1.3 and 2.4 which causes a denial of service (DOS) via a crafted web request.	2021-06-01	not yet calculated	CVE-2021-31684 MISC MISC MISC MISC
kde -- messagelib	KDE Messagelib through 5.17.0 reveals cleartext of encrypted messages in some situations. Deleting an attachment of a decrypted encrypted message stored on a remote server (e.g., an IMAP server) causes KMail to upload the decrypted content of the message to the remote server. With a crafted message, a user could be tricked into decrypting an encrypted message and then deleting an attachment attached to this message. If the attacker has access to the messages stored on the email server, then the attacker could read the decrypted content of the encrypted message. This occurs in ViewerPrivate::deleteAttachment in messageviewer/src/viewer/viewer_p.cpp.	2021-06-02	not yet calculated	CVE-2021-31855 MISC
kiali-operator -- kiali-operator	An incorrect access control flaw was found in the kiali-operator in versions before 1.33.0 and before 1.24.7. This flaw allows an attacker with a basic level of access to the cluster (to deploy a kiali operand) to use this vulnerability and deploy a given image to anywhere in the cluster, potentially gaining access to privileged service account tokens. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-06-01	not yet calculated	CVE-2021-3495 MISC MISC
lasso -- lasso	Lasso all versions prior to 2.7.0 has improper verification of a cryptographic signature.	2021-06-04	not yet calculated	CVE-2021-28091 MISC MISC MISC DEBIAN
libavcodec -- libavcodec	dwa_uncompress in libavcodec/exr.c in FFmpeg 4.4 allows an out-of-bounds array access because dc_count is not strictly checked.	2021-06-03	not yet calculated	CVE-2021-33815 MISC
libpeg-turbo -- libpeg-turbo	Libjpeg-turbo all version have a stack-based buffer overflow in the "transform" component. A remote attacker can send a malformed jpeg file to the service and cause arbitrary code execution or denial of service of the target service.	2021-06-01	not yet calculated	CVE-2020-17541 MISC
libraw -- libraw	Libraw before 0.20.1 has a stack buffer overflow via LibRaw::identify_process_dng_fields in identify.cpp.	2021-06-02	not yet calculated	CVE-2020-24870 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
libtpms -- libtpms	A stack corruption bug was found in libtpms in versions before 0.7.2 and before 0.8.0 while decrypting data using RSA. This flaw could result in a SIGBUS (bad memory access) and termination of swtpm. The highest threat from this vulnerability is to system availability.	2021-06-03	not yet calculated	CVE-2021-3569 MISC
libxml2 -- xmllint	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability.	2021-06-01	not yet calculated	CVE-2021-3516 MISC
linux -- linux_kernel	The io_uring subsystem in the Linux kernel allowed the MAX_RW_COUNT limit to be bypassed in the PROVIDE_BUFFERS operation, which led to negative values being usedin mem_rw when reading /proc/<PID>/mem. This could be used to create a heap overflow leading to arbitrary code execution in the kernel. It was addressed via commit d1f82808877b ("io_uring: truncate lengths larger than MAX_RW_COUNT on provide buffers") (v5.13-rc1) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced in ddf0322db79c ("io_uring: add IORING_OP_PROVIDE_BUFFERS") (v5.7-rc1).	2021-06-04	not yet calculated	CVE-2021-3491 UBUNTU UBUNTU MISC MISC MLIST
linux -- linux_kernel	A flaw was found in the Linux kernel. An index buffer overflow during Direct IO write leading to the NFS client to crash. In some cases, a reach out of the index after one memory allocation by kmalloc will cause a kernel panic. The highest threat from this vulnerability is to data confidentiality and system availability.	2021-06-02	not yet calculated	CVE-2020-10742 MISC
linux -- linux_kernel	The eBPF RINGBUF bpf_ringbuf_reserve() function in the Linux kernel did not check that the allocated size was smaller than the ringbuf size, allowing an attacker to perform out-of-bounds writes within the kernel and therefore, arbitrary code execution. This issue was fixed via commit 4b81ccebaeee ("bpf, ringbuf: Deny reserve of buffers larger than ringbuf") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced via 457f44363a88 ("bpf: Implement BPF ring buffer and verifier support for it") (v5.8-rc1).	2021-06-04	not yet calculated	CVE-2021-3489 MISC UBUNTU UBUNTU MISC MLIST
linux -- linux_kernel	The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel did not properly update 32-bit bounds, which could be turned into out of bounds reads and writes in the Linux kernel and therefore, arbitrary code execution. This issue was fixed via commit 049c4e13714e ("bpf: Fix alu32 const subreg bound tracking on bitwise operations") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. The AND/OR issues were introduced by commit 3f50f132d840 ("bpf: Verifier, do explicit ALU32 bounds tracking") (5.7-rc1) and the XOR variant was introduced by 2921c90d4718 ("bpf:Fix a verifier failure with xor") (5.10-rc1).	2021-06-04	not yet calculated	CVE-2021-3490 UBUNTU MISC MISC UBUNTU MLIST
luca -- luca	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because requests related to Check-In State occur shortly after requests for Phone Number Registration.	2021-06-04	not yet calculated	CVE-2021-33838 MISC MISC MISC MISC
luca -- luca	Luca through 1.7.4 on Android allows remote attackers to obtain sensitive information about COVID-19 tracking because the QR code of a Public Location can be intentionally confused with the QR code of a Private Meeting.	2021-06-04	not yet calculated	CVE-2021-33839 MISC MISC MISC MISC
luca -- luca	The server in Luca through 1.1.14 allows remote attackers to cause a denial of service (insertion of many fake records related to COVID-19) because Phone Number data lacks a digital signature.	2021-06-04	not yet calculated	CVE-2021-33840 MISC MISC
lz4 -- lz4	There's a flaw in lz4. An attacker who submits a crafted file to an application linked with lz4 may be able to trigger an integer overflow, leading to calling of memmove() on a negative size argument, causing an out-of-bounds write and/or a crash. The greatest impact of this flaw is to availability, with some potential impact to confidentiality and integrity as well.	2021-06-02	not yet calculated	CVE-2021-3520 MISC
mcafee -- database_security	Cleartext Transmission of Sensitive Information vulnerability in the administrator interface of McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to view the unencrypted password of the McAfee Insights Server used to pass data to the Insights Server. This user is restricted to only have access to DBSec data in the Insights Server.	2021-06-02	not yet calculated	CVE-2021-23896 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mcafee -- database_security	Incorrect access to deleted scripts vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote authenticated attacker to gain access to signed SQL scripts which have been marked as deleted or expired within the administrative console. This access was only available through the REST API.	2021-06-03	not yet calculated	CVE-2021-31831 CONFIRM
mcafee -- database_security	Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote authenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server.	2021-06-02	not yet calculated	CVE-2021-23895 CONFIRM
mcafee -- database_security	Deserialization of untrusted data vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows a remote unauthenticated attacker to create a reverse shell with administrator privileges on the DBSec server via carefully constructed Java serialized object sent to the DBSec server.	2021-06-02	not yet calculated	CVE-2021-23894 CONFIRM
mcafee -- database_security	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in McAfee Database Security (DBSec) prior to 4.8.2 allows an administrator to embed JavaScript code when configuring the name of a database to be monitored. This would be triggered when any authorized user logs into the DBSec interface and opens the properties configuration page for this database.	2021-06-03	not yet calculated	CVE-2021-31830 CONFIRM
micro_focus -- secure_api_manager	Insertion of Sensitive Information into Log File vulnerability in Micro Focus Secure API Manager (SAPIM) product, affecting version 2.0.0. The vulnerability could lead to sensitive information being in a log file.	2021-06-04	not yet calculated	CVE-2021-22516 MISC
micrologix -- micrologix	When an authenticated password change request takes place, this vulnerability could allow the attacker to intercept the message that includes the legitimate, new password hash and replace it with an illegitimate hash. The user would no longer be able to authenticate to the controller (Micro800: All versions, MicroLogix 1400: Version 21 and later) causing a denial-of-service condition	2021-06-03	not yet calculated	CVE-2021-32926 MISC
mintty -- mintty	Mintty before 3.4.5 allows remote servers to cause a denial of service (Windows GUI hang) by telling the Mintty window to change its title repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls. In other words, it does not implement a usleep or similar delay upon processing a title change.	2021-06-03	not yet calculated	CVE-2021-28848 CONFIRM MISC CONFIRM
mobaxterm -- mobaxterm	MobaXterm before 21.0 allows remote servers to cause a denial of service (Windows GUI hang) via tab title change requests that are sent repeatedly at high speed, which results in many SetWindowTextA or SetWindowTextW calls.	2021-06-03	not yet calculated	CVE-2021-28847 MISC CONFIRM
mozilla -- firefox	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 3.6.24 and 4.x through 7 allows remote attackers to inject arbitrary web script or HTML via vectors involving HTTP 0.9 errors, non-default ports, and content-sniffing.	2021-06-02	not yet calculated	CVE-2011-3656 MISC
mozilla -- thunderbird	A flaw was found in the xdg-email component of xdg-utils-1.1.0-rc1 and newer. When handling mailto: URIs, xdg-email allows attachments to be discreetly added via the URI when being passed to Thunderbird. An attacker could potentially send a victim a URI that automatically attaches a sensitive file to a new email. If a victim user does not notice that an attachment was added and sends the email, this could result in sensitive information disclosure. It has been confirmed that the code behind this issue is in xdg-email and not in Thunderbird.	2021-06-01	not yet calculated	CVE-2020-27748 MISC MISC
nestie -- nestie	Prototype pollution vulnerability in 'nestie' versions 0.0.0 through 1.0.0 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-06-03	not yet calculated	CVE-2021-25947 MISC
nextcloud -- mail	Nextcloud Mail is a mail app for the Nextcloud platform. A missing permission check in Nextcloud Mail before 1.4.3 and 1.8.2 allows another authenticated users to access mail metadata of other users. Versions 1.4.3 and 1.8.2 contain patches for this vulnerability; no workarounds other than the patches are known to exist.	2021-06-01	not yet calculated	CVE-2021-32652 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- server	Nextcloud Server is a Nextcloud package that handles data storage. A vulnerability in federated share exists in versions prior to 19.0.11, 20.0.10, and 21.0.2. An attacker can gain access to basic information about users of a server by accessing a public link that a legitimate server user added as a federated share. This happens because Nextcloud supports sharing registered users with other Nextcloud servers, which can be done automatically when selecting the "Add server automatically once a federated share was created successfully" setting. The vulnerability is patched in versions 19.0.11, 20.0.10, and 21.0.2 As a workaround, disable "Add server automatically once a federated share was created successfully" in the Nextcloud settings.	2021-06-01	not yet calculated	CVE-2021-32656 MISC CONFIRM
nextcloud -- server	Nextcloud Server is a Nextcloud package that handles data storage. In versions of Nextcloud Server prior to 10.0.11, 20.0.10, and 21.0.2, a malicious user may be able to break the user administration page. This would disallow administrators to administrate users on the Nextcloud instance. The vulnerability is fixed in versions 19.0.11, 20.0.10, and 21.0.2. As a workaround, administrators can use the OCC command line tool to administrate the Nextcloud users.	2021-06-01	not yet calculated	CVE-2021-32657 MISC CONFIRM
nextcloud -- server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.11, 20.0.10, and 21.0.2, an attacker is able to convert a Files Drop link to a federated share. This causes an issue on the UI side of the sharing user. When the sharing user opens the sharing panel and tries to remove the "Create" privileges of this unexpected share, Nextcloud server would silently grant the share read privileges. The vulnerability is patched in versions 19.0.11, 20.0.10 and 21.0.2. No workarounds are known to exist.	2021-06-01	not yet calculated	CVE-2021-32655 MISC CONFIRM
nextcloud -- server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.11, 20.0.10, and 21.0.2, an attacker is able to receive write/read privileges on any Federated File Share. Since public links can be added as federated file share, this can also be exploited on any public link. Users can upgrade to patched versions (19.0.11, 20.0.10 or 21.0.2) or, as a workaround, disable federated file sharing.	2021-06-01	not yet calculated	CVE-2021-32654 CONFIRM MISC
nextcloud -- server	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server versions prior to 19.0.11, 20.0.10, or 21.0.2 send user IDs to the lookup server even if the user has no fields set to published. The vulnerability is patched in versions 19.0.11, 20.0.10, and 21.0.2; no workarounds outside the updates are known to exist.	2021-06-01	not yet calculated	CVE-2021-32653 MISC CONFIRM
ngix -- controller	The NGINX Controller 2.0.0 thru 2.9.0 and 3.x before 3.15.0 Administrator password may be exposed in the systemd.txt file that is included in the NGINX support package.	2021-06-01	not yet calculated	CVE-2021-23019 MISC
ngix -- controller	The NAAS 3.x before 3.10.0 API keys were generated using an insecure pseudo-random string and hashing algorithm which could lead to predictable keys.	2021-06-01	not yet calculated	CVE-2021-23020 MISC
ngix -- controller	The package forms before 1.2.1, from 1.3.0 and before 1.3.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via email validation.	2021-06-01	not yet calculated	CVE-2021-23388 MISC MISC MISC
ngix -- controller	Intra-cluster communication does not use TLS. The services within the NGINX Controller 3.x before 3.4.0 namespace are using cleartext protocols inside the cluster.	2021-06-01	not yet calculated	CVE-2021-23018 MISC
ngix -- controller	The Nginx Controller 3.x before 3.7.0 agent configuration file /etc/controller-agent/agent.conf is world readable with current permission bits set to 644.	2021-06-01	not yet calculated	CVE-2021-23021 MISC
ngix -- resolver	A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.	2021-06-01	not yet calculated	CVE-2021-23017 MISC MISC
nitro_enclaves -- kernel_driver	A flaw null pointer dereference in the Nitro Enclaves kernel driver was found in the way that Enclaves VMs forces closures on the enclave file descriptor. A local user of a host machine could use this flaw to crash the system or escalate their privileges on the system.	2021-06-01	not yet calculated	CVE-2021-3543 MISC MISC
node.js -- merge-deep-library	The merge-deep library before 3.0.3 for Node.js can be tricked into overwriting properties of Object.prototype or adding new properties to it. These properties are then inherited by every object in the program, thus facilitating prototype-pollution attacks against applications using this library.	2021-06-02	not yet calculated	CVE-2021-26707 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
noobaa-core -- noobaa-core	A flaw was found in noobaa-core in versions before 5.7.0. This flaw results in the name of an arbitrarily URL being copied into an HTML document as plain text between tags, including potentially a payload script. The input was echoed unmodified in the application response, resulting in arbitrary JavaScript being injected into an application's response. The highest threat to the system is for confidentiality, availability, and integrity.	2021-06-02	not yet calculated	CVE-2021-3529 MISC
obottle -- obottle	OBottle 2.0 in \c\t.php contains an arbitrary file write vulnerability.	2021-06-03	not yet calculated	CVE-2020-36008 CONFIRM
obottle -- obottle	OBottle 2.0 in \c\g.php contains an arbitrary file download vulnerability.	2021-06-03	not yet calculated	CVE-2020-36009 CONFIRM
onedev -- onedev	OneDev is a development operations platform. If the LDAP external authentication mechanism is enabled in OneDev versions 4.4.1 and prior, an attacker can manipulate a user search filter to send forged queries to the application and explore the LDAP tree using Blind LDAP Injection techniques. The specific payload depends on how the User Search Filter property is configured in OneDev. This issue was fixed in version 4.4.2.	2021-06-01	not yet calculated	CVE-2021-32651 MISC CONFIRM
online_shopping_alphaware -- online_shopping_alphaware	The id paramater in Online Shopping Alphaware 1.0 has been discovered to be vulnerable to an Error-Based blind SQL injection in the /alphaware/details.php path. This allows an attacker to retrieve all databases.	2021-06-02	not yet calculated	CVE-2020-25362 MISC MISC MISC
opennms -- horizon	In OpenNMS Horizon, versions opennms-1-0-stable through opennms-27.1.0-1; OpenNMS Meridian, versions meridian-foundation-2015.1.0-1 through meridian-foundation-2019.1.18-1; meridian-foundation-2020.1.0-1 through meridian-foundation-2020.1.6-1 are vulnerable to Stored Cross-Site Scripting, since the function `validateFormInput()` performs improper validation checks on the input sent to the `userID` parameter. Due to this flaw an attacker could inject an arbitrary script which will be stored in the database.	2021-06-01	not yet calculated	CVE-2021-25932 MISC MISC MISC MISC
openshift -- container_platform	A flaw was found in the Restricted Security Context Constraints (SCC), where it allows pods to craft custom network packets. This flaw allows an attacker to cause a denial of service attack on an OpenShift Container Platform cluster if they can deploy pods. The highest threat from this vulnerability is to system availability.	2021-06-02	not yet calculated	CVE-2020-14336 MISC
openshift -- container_platform	It was discovered that OpenShift Container Platform's (OCP) distribution of Kibana could open in an iframe, which made it possible to intercept and manipulate requests. This flaw allows an attacker to trick a user into performing arbitrary actions in OCP's distribution of Kibana, such as clickjacking.	2021-06-02	not yet calculated	CVE-2020-10743 MISC
openshift -- openshift	An insecure modification flaw in the /etc/kubernetes/kubeconfig file was found in OpenShift. This flaw allows an attacker with access to a running container which mounts /etc/kubernetes or has local access to the node, to copy this kubeconfig file and attempt to add their own node to the OpenShift cluster. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. This flaw affects versions before openshift4/ose-machine-config-operator v4.7.0-202105111858.p0.	2021-06-02	not yet calculated	CVE-2020-35514 MISC
openstack -- swift	In OpenStack Swift through 2.10.1, 2.11.0 through 2.13.0, and 2.14.0, the proxy-server logs full tempurl paths, potentially leaking reusable tempurl signatures to anyone with read access to these logs. All Swift deployments using the tempurl middleware are affected.	2021-06-02	not yet calculated	CVE-2017-8761 MISC
openvpn -- access_server	OpenVPN Access Server 2.8.7 and earlier versions allows a remote attackers to bypass authentication and access control channel data on servers configured with deferred authentication, which can be used to potentially trigger further information leaks.	2021-06-04	not yet calculated	CVE-2020-15077 MISC MISC
openvpn -- access_server	OpenVPN Access Server 2.7.3 to 2.8.7 allows remote attackers to trigger an assert during the user authentication phase via incorrect authentication token data in an early phase of the user authentication resulting in a denial of service.	2021-06-04	not yet calculated	CVE-2020-36382 MISC MISC
ovn -- kubernetes	A vulnerability was found in OVN Kubernetes in versions up to and including 0.3.0 where the Egress Firewall does not reliably apply firewall rules when there is multiple DNS rules. It could lead to potentially lose of confidentiality, integrity or availability of a service.	2021-06-02	not yet calculated	CVE-2021-3499 MISC
pbootcms -- pbootcms	Pbootcms v2.0.3 is vulnerable to Cross Site Scripting (XSS) via admin.php.	2021-06-03	not yet calculated	CVE-2020-21003 MISC
pfsense -- pfsense	A stored cross-site scripting (XSS) vulnerability was discovered in pfSense 2.4.5-p1 which allows an authenticated attacker to execute arbitrary web scripts via exploitation of the load_balancer_monitor.php function.	2021-06-01	not yet calculated	CVE-2020-26693 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pglogical -- pglocgical	A shell injection flaw was found in pglogical in versions before 2.3.4 and before 3.6.26. An attacker with CREATEDB privileges on a PostgreSQL server can craft a database name that allows execution of shell commands as the postgresql user when calling pglogical.create_subscription().	2021-06-01	not yet calculated	CVE-2021-3515 MISC
pharmacy_medical_store_and_sale_point -- pharmacy_medical_store_and_sale_point	The catID parameter in Pharmacy Medical Store and Sale Point v1.0 has been found to be vulnerable to a Time-Based blind SQL injection via the /medical/inventories.php path which allows attackers to retrieve all databases.	2021-06-02	not yet calculated	CVE-2020-24862 MISC MISC MISC
pillow -- pillow	An issue was discovered in Pillow before 8.2.0. For BLP data, BlpImagePlugin did not properly check that reads (after jumping to file offsets) returned data. This could lead to a DoS where the decoder could be run a large number of times on empty data.	2021-06-02	not yet calculated	CVE-2021-28678 MISC MISC FEDORA
pillow -- pillow	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_gray_i.	2021-06-02	not yet calculated	CVE-2021-25288 MISC MISC FEDORA
pillow -- pillow	An issue was discovered in Pillow before 8.2.0. For FLI data, FliDecode did not properly check that the block advance was non-zero, potentially leading to an infinite loop on load.	2021-06-02	not yet calculated	CVE-2021-28676 MISC MISC FEDORA
pillow -- pillow	An issue was discovered in Pillow before 8.2.0. PSDImagePlugin.PsdImageFile lacked a sanity check on the number of input layers relative to the size of the data block. This could lead to a DoS on Image.open prior to Image.load.	2021-06-02	not yet calculated	CVE-2021-28675 MISC FEDORA
pillow -- pillow	An issue was discovered in Pillow before 8.2.0. For EPS data, the readline implementation used in EPSImageFile has to deal with any combination of \r and \n as line endings. It used an accidentally quadratic method of accumulating lines while looking for a line ending. A malicious EPS file could use this to perform a DoS of Pillow in the open phase, before an image was accepted for opening.	2021-06-02	not yet calculated	CVE-2021-28677 MISC MISC FEDORA
pillow -- pillow	An issue was discovered in Pillow before 8.2.0. There is an out-of-bounds read in J2kDecode, in j2ku_graya_la.	2021-06-02	not yet calculated	CVE-2021-25287 MISC MISC FEDORA
postgresql -- postgresql	A flaw was found in postgresql in versions before 13.3, before 12.7, before 11.12, before 10.17 and before 9.6.22. While modifying certain SQL array values, missing bounds checks let authenticated database users write arbitrary bytes to a wide area of server memory. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-06-01	not yet calculated	CVE-2021-32027 MISC MISC
qemu -- qemu	Several memory leaks were found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and including 6.0. They exist in contrib/vhost-user-gpu/vhost-user-gpu.c and contrib/vhost-user-gpu/virgl.c due to improper release of memory (i.e., free) after effective lifetime.	2021-06-02	not yet calculated	CVE-2021-3544 MISC MLIST
qemu -- qemu	A flaw was found in vhost-user-gpu of QEMU in versions up to and including 6.0. An out-of-bounds write vulnerability can allow a malicious guest to crash the QEMU process on the host resulting in a denial of service or potentially execute arbitrary code on the host with the privileges of the QEMU process. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	2021-06-02	not yet calculated	CVE-2021-3546 MISC MLIST
qemu -- qemu	A NULL pointer dereference flaw was found in the megasas-gen2 SCSI host bus adapter emulation of QEMU in versions before and including 6.0. This issue occurs in the megasas_command_cancelled() callback function while dropping a SCSI request. This flaw allows a privileged guest user to crash the QEMU process on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	2021-06-02	not yet calculated	CVE-2020-35503 MISC
qemu -- qemu	An information disclosure vulnerability was found in the virtio vhost-user GPU device (vhost-user-gpu) of QEMU in versions up to and including 6.0. The flaw exists in virgl_cmd_get_capset_info() in contrib/vhost-user-gpu/virgl.c and could occur due to the read of uninitialized memory. A malicious guest could exploit this issue to leak memory from the host.	2021-06-02	not yet calculated	CVE-2021-3545 MISC MLIST
qemu -- qemu	A divide-by-zero issue was found in dwc2_handle_packet in hw/usb/hcd-dwc2.c in the hcd-dwc2 USB host controller emulation of QEMU. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service.	2021-06-02	not yet calculated	CVE-2020-27661 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qemu -- qemu	The ahci_commit_buf function in ide/ahci.c in QEMU allows attackers to cause a denial of service (NULL dereference) when the command header 'ad->cur_cmd' is null.	2021-06-02	not yet calculated	CVE-2019-12067 MISC MISC MISC MISC
qnap -- nas	A DOM-based XSS vulnerability has been reported to affect QNAP NAS running QTS and QuTS hero. If exploited, this vulnerability allows attackers to inject malicious code. This issue affects: QNAP Systems Inc. QTS versions prior to 4.5.3.1652 Build 20210428. QNAP Systems Inc. QuTS hero versions prior to h4.5.2.1638 Build 20210414. QNAP Systems Inc. QuTScloud versions prior to c4.5.5.1656 Build 20210503. This issue does not affect: QNAP Systems Inc. QTS 4.3.6; 4.3.3.	2021-06-03	not yet calculated	CVE-2021-28806 MISC
qnap -- nas	A post-authentication reflected XSS vulnerability has been reported to affect QNAP NAS running Q'center. If exploited, this vulnerability allows remote attackers to inject malicious code. QNAP have already fixed this vulnerability in the following versions of Q'center: QTS 4.5.3: Q'center v1.12.1012 and later QTS 4.3.6: Q'center v1.10.1004 and later QTS 4.3.3: Q'center v1.10.1004 and later QuTS hero h4.5.2: Q'center v1.12.1012 and later QuTScloud c4.5.4: Q'center v1.12.1012 and later	2021-06-03	not yet calculated	CVE-2021-28807 MISC
qnap -- video_station	A command injection vulnerability has been reported to affect certain versions of Video Station. If exploited, this vulnerability allows remote attackers to execute arbitrary commands. This issue affects: QNAP Systems Inc. Video Station versions prior to 5.5.4 on QTS 4.5.2; versions prior to 5.5.4 on QuTS hero h4.5.2; versions prior to 5.5.4 on QuTScloud c4.5.4. This issue does not affect: QNAP Systems Inc. Video Station on QTS 4.3.6; on QTS 4.3.3.	2021-06-03	not yet calculated	CVE-2021-28812 MISC
realtek -- rtl8710	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices) can lead to remote code execution via the "memcpy" function, when an attacker in Wi-Fi range sends a crafted "Encrypted GTK" value as part of the WPA2 4-way-handshake.	2021-06-04	not yet calculated	CVE-2020-27302 MISC
realtek -- rtl8710	A stack buffer overflow in Realtek RTL8710 (and other Ameba-based devices) can lead to remote code execution via the "AES_UnWRAP" function, when an attacker in Wi-Fi range sends a crafted "Encrypted GTK" value as part of the WPA2 4-way-handshake.	2021-06-04	not yet calculated	CVE-2020-27301 MISC
reborncore -- library	The RebornCore library before 4.7.3 allows remote code execution because it deserializes untrusted data in ObjectInputStream.readObject as part of reborncore.common.network.ExtendedPacketBuffer. An attacker can instantiate any class on the classpath with any data. A class usable for exploitation might or might not be present, depending on what Minecraft modifications are installed.	2021-05-31	not yet calculated	CVE-2021-33790 MISC MISC MISC
red_hat -- red_hat	A flaw was found in keycloak as shipped in Red Hat Single Sign-On 7.4 where IDN homograph attacks are possible. A malicious user can register himself with a name already registered and trick admin to grant him extra privileges.	2021-06-01	not yet calculated	CVE-2021-3424 MISC
red_hat -- red_hat	A flaw was found in the AMQ Broker that discloses JDBC encrypted usernames and passwords when provided in the AMQ Broker application logfile when using the jdbc persistence functionality. Versions shipped in Red Hat AMQ 7 are vulnerable.	2021-06-01	not yet calculated	CVE-2021-3425 MISC
red_hat -- red_hat	An account takeover flaw was found in Red Hat Satellite 6.7.2 onward. A potential attacker with proper authentication to the relevant external authentication source (SSO or Open ID) can claim the privileges of already existing local users of Satellite.	2021-06-02	not yet calculated	CVE-2020-14380 MISC
red_hat -- red_hat	A credential leak vulnerability was found in Red Hat Satellite. This flaw exposes the compute resources credentials through VMs that are running on these resources in Satellite.	2021-06-02	not yet calculated	CVE-2020-14371 MISC
red_hat -- red_hat	A flaw was found in the Red Hat 3scale API Management Platform, where member permissions for an API's admin portal were not properly enforced. This flaw allows an authenticated user to bypass normal account restrictions and access API services where they do not have permission.	2021-06-02	not yet calculated	CVE-2020-14388 MISC
red_hat -- red_hat	A flaw was found in Red Hat Satellite, which allows a privileged attacker to read OMAPI secrets through the ISC DHCP of Smart-Proxy. This flaw allows an attacker to gain control of DHCP records from the network. The highest threat from this vulnerability is to system availability.	2021-06-02	not yet calculated	CVE-2020-14335 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
redis -- redis	Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache, and message broker. An integer overflow bug in Redis version 6.0 or newer (on 32-bit systems ONLY) can be exploited using the `STRALGO LCS` command to corrupt the heap and potentially result with remote code execution. This is a result of an incomplete fix for CVE-2021-29477 which only addresses the problem on 64-bit systems but fails to do that for 32-bit. 64-bit systems are not affected. The problem is fixed in version 6.2.4 and 6.0.14. An additional workaround to mitigate the problem without patching the `redis-server` executable is to use ACL configuration to prevent clients from using the `STRALGO LCS` command.	2021-06-02	not yet calculated	CVE-2021-32625 CONFIRM MISC MISC
resteasy -- resteasy	A vulnerability was found in RESTEasy, where RootNode incorrectly caches routes. This issue results in hash flooding, leading to slower requests with higher CPU time spent searching and adding the entry. This flaw allows an attacker to cause a denial of service.	2021-06-02	not yet calculated	CVE-2020-14326 MISC
ruby -- dragonfly	An argument injection vulnerability in the Dragonfly gem before 1.4.0 for Ruby allows remote attackers to read and write to arbitrary files via a crafted URL when the verify_url option is disabled. This may lead to code execution. The problem occurs because the generate and process features mishandle use of the ImageMagick convert utility.	2021-05-29	not yet calculated	CVE-2021-33564 MISC MISC MISC MISC MISC MISC
rust -- deno	Deno is a runtime for JavaScript and TypeScript that uses V8 and is built in Rust. In Deno versions 1.5.0 to 1.10.1, modules that are dynamically imported through `import()` or `new Worker` might have been able to bypass network and file system permission checks when statically importing other modules. The vulnerability has been patched in Deno release 1.10.2.	2021-05-28	not yet calculated	CVE-2021-32619 CONFIRM
sangoma -- freepbx_and_pbxact	The restapps (aka Rest Phone apps) module for Sangoma FreePBX and PBXact 13, 14, and 15 through 15.0.19.2 allows remote code execution via a URL variable to an AMI command.	2021-05-31	not yet calculated	CVE-2020-10666 MISC MISC
singularity -- singularity	### Impact Due to incorrect use of a default URL, `singularity` action commands (`run`/`shell`/`exec`) specifying a container using a `library://` URI will always attempt to retrieve the container from the default remote endpoint (`cloud.sylabs.io`) rather than the configured remote endpoint. An attacker may be able to push a malicious container to the default remote endpoint with a URI that is identical to the URI used by a victim with a non-default remote endpoint, thus executing the malicious container. Only action commands (`run`/`shell`/`exec`) against `library://` URIs are affected. Other commands such as `pull` / `push` respect the configured remote endpoint. ### Patches All users should upgrade to Singularity 3.7.4 or later. ### Workarounds Users who only interact with the default remote endpoint are not affected. Installations with an execution control list configured to restrict execution to containers signed with specific secure keys are not affected. ### For more information General questions about the impact of the advisory can be asked in the: - [SingularityCE Slack Channel](https://singularityce.slack.com) - [SingularityCE Mailing List](https://groups.google.com/g/singularity-ce) Any sensitive security concerns should be directed to: security@sylabs.io See our Security Policy here: https://sylabs.io/security-policy	2021-05-28	not yet calculated	CVE-2021-32635 CONFIRM
sogo -- sogo	SOGo 2.x before 2.4.1 and 3.x through 5.x before 5.1.1 does not validate the signatures of any SAML assertions it receives. Any actor with network access to the deployment could impersonate users when SAML is the authentication method. (Only versions after 2.0.5a are affected.)	2021-06-04	not yet calculated	CVE-2021-33054 MISC MISC MISC
synology -- diskstation_manager	Improper limitation of a pathname to a restricted directory ('Path Traversal') in cgi component in Synology DiskStation Manager (DSM) before 6.2.4-25553 allows local users to execute arbitrary code via unspecified vectors.	2021-06-01	not yet calculated	CVE-2021-29088 CONFIRM
synology -- docker	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability container volume management component in Synology Docker before 18.09.0-0515 allows local users to read or write arbitrary files via unspecified vectors.	2021-06-01	not yet calculated	CVE-2021-33183 CONFIRM
synology -- download_station	Server-Side request forgery (SSRF) vulnerability in task management component in Synology Download Station before 3.8.15-3563 allows remote authenticated users to read arbitrary files via unspecified vectors.	2021-06-01	not yet calculated	CVE-2021-33184 CONFIRM
synology -- photo_station	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in file management component in Synology Photo Station before 6.8.14-3500 allows remote authenticated users to write arbitrary files via unspecified vectors.	2021-06-02	not yet calculated	CVE-2021-29091 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
synology -- photo_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in thumbnail component in Synology Photo Station before 6.8.14-3500 allows remote attackers users to execute arbitrary SQL commands via unspecified vectors.	2021-06-02	not yet calculated	CVE-2021-29089 CONFIRM
synology -- photo_station	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in PHP component in Synology Photo Station before 6.8.14-3500 allows remote authenticated users to execute arbitrary SQL command via unspecified vectors.	2021-06-02	not yet calculated	CVE-2021-29090 CONFIRM
synology -- photo_station	Unrestricted upload of file with dangerous type vulnerability in file management component in Synology Photo Station before 6.8.14-3500 allows remote authenticated users to execute arbitrary code via unspecified vectors.	2021-06-01	not yet calculated	CVE-2021-29092 CONFIRM
synology -- diskstation_manager	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in PDF Viewer component in Synology DiskStation Manager (DSM) before 6.2.4-25553 allows remote authenticated users to read limited files via unspecified vectors.	2021-06-01	not yet calculated	CVE-2021-33182 CONFIRM
synology -- media_server	Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in cgi component in Synology Media Server before 1.8.1-2876 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2021-06-01	not yet calculated	CVE-2021-33180 CONFIRM
synology -- video_station	Server-Side Request Forgery (SSRF) vulnerability in webapi component in Synology Video Station before 2.4.10-1632 allows remote authenticated users to send arbitrary request to intranet resources via unspecified vectors.	2021-06-01	not yet calculated	CVE-2021-33181 CONFIRM
tianocore -- edk2	Null pointer dereference in Tianocore EDK2 may allow an authenticated user to potentially enable escalation of privilege via local access.	2021-06-03	not yet calculated	CVE-2019-14584 MISC
tpm2-tools -- tpm2-tools	A flaw was found in tpm2-tools in versions before 5.1.1 and before 4.3.2. tpm2_import used a fixed AES key for the inner wrapper, potentially allowing a MITM attacker to unwrap the inner portion and reveal the key being imported. The highest threat from this vulnerability is to data confidentiality.	2021-06-04	not yet calculated	CVE-2021-3565 MISC
trend_micro -- maximum_security	The Trend Micro Maximum Security 2021 (v17) consumer product is vulnerable to an improper access control vulnerability in the installer which could allow a local attacker to escalate privileges on a target machine. Please note than an attacker must already have local user privileges and access on the machine to exploit this vulnerability.	2021-06-03	not yet calculated	CVE-2021-32460 MISC MISC
validatebaseurl -- validatebaseurl	A regular expression denial of service (ReDoS) vulnerability in the validateBaseUrl function can cause the application to use excessive resources, become unresponsive, or crash. This was introduced in react-native version 0.59.0 and fixed in version 0.64.1.	2021-06-01	not yet calculated	CVE-2020-1920 CONFIRM MISC
vmware -- vcenter	A security vulnerability in HPE OneView for VMware vCenter (OV4VC) could be exploited remotely to allow Cross-Site Scripting. HPE has released the following software update to resolve the vulnerability in HPE OneView for VMware vCenter (OV4VC).	2021-06-03	not yet calculated	CVE-2021-26584 MISC
volpmonitor -- volpmonitor	A remote code execution issue was discovered in the web UI of VoIPmonitor before 24.61. When the recheck option is used, the user-supplied SPOOLDIR value (which might contain PHP code) is injected into config/configuration.php.	2021-05-29	not yet calculated	CVE-2021-30461 MISC
wellcms -- wellcms	WellCMS 2.0 beta3 is vulnerable to File Upload. A user can log in to the CMS background and upload a picture. Because the upload file type is controllable, the user can modify the upload file type to get webshell.	2021-06-03	not yet calculated	CVE-2020-21005 MISC MISC
wire -- iore-ios	wire-ios is the iOS version of Wire, an open-source secure messaging app. In wire-ios versions 3.8.0 and prior, a vulnerability exists that can cause a denial of service between users. If a user has an invalid assetID for their profile picture and it contains the " character, it will cause the iOS client to crash. The vulnerability is patched in wire-ios version 3.8.1.	2021-06-03	not yet calculated	CVE-2021-32666 CONFIRM MISC
wire -- iore-ios	wire-ios is the iOS version of Wire, an open-source secure messaging app. wire-ios versions 3.8.0 and earlier have a bug in which a conversation could be incorrectly set to "unverified. This occurs when: - Self user is added to a new conversation - Self user is added to an existing conversation - All the participants in the conversation were previously marked as verified. The vulnerability is patched in wire-ios version 3.8.1. As a workaround, one can unverify & verify a device in the conversation.	2021-06-03	not yet calculated	CVE-2021-32665 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Instant Images â€“ One Click Unsplash Uploads WordPress plugin before 4.4.0.1 did not properly validate and sanitise its unsplash_download_w and unsplash_download_h parameter settings (/wp-admin/upload.php?page=instant-images), only validating them client side before saving them, leading to a Stored Cross-Site Scripting issue.	2021-06-01	not yet calculated	CVE-2021-24334 MISC CONFIRM
wordpress -- wordpress	The WP Login Security and History WordPress plugin through 1.0 did not have CSRF check when saving its settings, not any sanitisation or validation on them. This could allow attackers to make logged in administrators change the plugin's settings to arbitrary values, and set XSS payloads on them as well	2021-06-01	not yet calculated	CVE-2021-24328 MISC MISC CONFIRM MISC
wordpress -- wordpress	The WP Prayer WordPress plugin before 1.6.2 provides the functionality to store requested prayers/praises and list them on a WordPress website. These stored prayer/praise requests can be listed by using the WP Prayer engine. An authenticated WordPress user with any role can fill in the form to request a prayer. The form to request prayers or praises have several fields. The 'prayer request' and 'praise request' fields do not use proper input validation and can be used to store XSS payloads.	2021-06-01	not yet calculated	CVE-2021-24313 CONFIRM
wordpress -- wordpress	The wp_ajax_upload-remote-file AJAX action of the External Media WordPress plugin before 1.0.34 was vulnerable to arbitrary file uploads via any authenticated users.	2021-06-01	not yet calculated	CVE-2021-24311 CONFIRM MISC
wordpress -- wordpress	The WP Super Cache WordPress plugin before 1.7.3 did not properly sanitise its wp_cache_location parameter in its settings, which could lead to a Stored Cross-Site Scripting issue.	2021-06-01	not yet calculated	CVE-2021-24329 CONFIRM MISC
wordpress -- wordpress	The Funnel Builder by CartFlows â€“ Create High Converting Sales Funnels For WordPress plugin before 1.6.13 did not sanitise its facebook_pixel_id and google_analytics_id settings, allowing high privilege users to set XSS payload in them, which will either be executed on pages generated by the plugin, or the whole website depending on the settings used.	2021-06-01	not yet calculated	CVE-2021-24330 CONFIRM MISC
wordpress -- wordpress	The Smooth Scroll Page Up/Down Buttons WordPress plugin before 1.4 did not properly sanitise and validate its settings, such as psb_distance, psb_buttonsize, psb_speed, only validating them client side. This could allow high privilege users (such as admin) to set XSS payloads in them	2021-06-01	not yet calculated	CVE-2021-24331 CONFIRM MISC
wordpress -- wordpress	The Content Copy Protection & Prevent Image Save WordPress plugin through 1.3 does not check for CSRF when saving its settings, not perform any validation and sanitisation on them, allowing attackers to make a logged in administrator set arbitrary XSS payloads in them.	2021-06-01	not yet calculated	CVE-2021-24333 MISC MISC CONFIRM MISC
wordpress -- wordpress	The Car Repair Services & Auto Mechanic WordPress theme before 4.0 did not properly sanitise its serviceestimatekey search parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting issue	2021-06-01	not yet calculated	CVE-2021-24335 MISC MISC CONFIRM
wordpress -- wordpress	The Bello - Directory & Listing WordPress theme before 1.6.0 did not properly sanitise its post_excerpt parameter before outputting it back in the shop/my-account/bello-listing-endpoint/ page, leading to a Cross-Site Scripting issue	2021-06-01	not yet calculated	CVE-2021-24319 MISC CONFIRM
wordpress -- wordpress	The search feature of the Mediumish WordPress theme through 1.0.47 does not properly sanitise it's 's' GET parameter before output it back the page, leading to the Cross-SIte Scripting issue.	2021-06-01	not yet calculated	CVE-2021-24316 MISC MISC CONFIRM
wordpress -- wordpress	The Database Backup for WordPress plugin before 2.4 did not escape the backup_recipient POST parameter in before output it back in the attribute of an HTML tag, leading to a Stored Cross-Site Scripting issue.	2021-06-01	not yet calculated	CVE-2021-24322 MISC CONFIRM
wordpress -- wordpress	The Bello - Directory & Listing WordPress theme before 1.6.0 did not sanitise the bt_bb_listing_field_price_range_to, bt_bb_listing_field_now_open, bt_bb_listing_field_my_lng, listing_list_view and bt_bb_listing_field_my_lat parameters before using them in a SQL statement, leading to SQL Injection issues	2021-06-01	not yet calculated	CVE-2021-24321 CONFIRM MISC
wordpress -- wordpress	The Bello - Directory & Listing WordPress theme before 1.6.0 did not properly sanitise and escape its listing_list_view, bt_bb_listing_field_my_lat, bt_bb_listing_field_my_lng, bt_bb_listing_field_distance_value, bt_bb_listing_field_my_lat_default, bt_bb_listing_field_keyword, bt_bb_listing_field_location_autocomplete, bt_bb_listing_field_price_range_from and bt_bb_listing_field_price_range_to parameter in ints listing page, leading to reflected Cross-Site Scripting issues.	2021-06-01	not yet calculated	CVE-2021-24320 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	The Listeo WordPress theme before 1.6.11 did not ensure that the Post/Page and Booking to delete belong to the user making the request, allowing any authenticated users to delete arbitrary page/post and booking via an IDOR vector.	2021-06-01	not yet calculated	CVE-2021-24318 CONFIRM MISC
wordpress -- wordpress	The Listeo WordPress theme before 1.6.11 did not properly sanitise some parameters in its Search, Booking Confirmation and Personal Message pages, leading to Cross-Site Scripting issues	2021-06-01	not yet calculated	CVE-2021-24317 MISC CONFIRM
wordpress -- wordpress	The parameters $cache_path, $wp_cache_debug_ip, $wp_super_cache_front_page_text, $cache_scheduled_time, $cached_direct_pages used in the settings of WP Super Cache WordPress plugin before 1.7.3 result in RCE because they allow input of '$' and '\n'. This is due to an incomplete fix of CVE-2021-24209.	2021-06-01	not yet calculated	CVE-2021-24312 CONFIRM
wordpress -- wordpress	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery WordPress plugin before 1.5.67 did not properly sanitise the gallery title, allowing high privilege users to create one with XSS payload in it, which will be triggered when another user will view the gallery list or the affected gallery in the admin dashboard. This is due to an incomplete fix of CVE-2019-16117	2021-06-01	not yet calculated	CVE-2021-24310 CONFIRM
wordpress -- wordpress	The "Schedule Name" input in the Weekly Schedule WordPress plugin before 3.4.3 general options did not properly sanitize input, allowing a user to inject javascript code using the <script> HTML tags and cause a stored XSS issue	2021-06-01	not yet calculated	CVE-2021-24309 CONFIRM
xnio -- xnio	A vulnerability was discovered in XNIO where file descriptor leak caused by growing amounts of NIO Selector file handles between garbage collection cycles. It may allow the attacker to cause a denial of service. It affects XNIO versions 3.6.0.Beta1 through 3.8.1.Final.	2021-06-02	not yet calculated	CVE-2020-14340 MISC
xstream -- xstream	### Impact The vulnerability may allow a remote attacker has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. ### Patches If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.17. ### Workarounds See [workarounds](https://x-stream.github.io/security.html#workaround) for the different versions covering all CVEs. ### References See full information about the nature of the vulnerability and the steps to reproduce it in XStream's documentation for [CVE-2021-xxxxx](https://x-stream.github.io/CVE-2021-xxxxx.html). ### Credits V3geB1rd, white hat hacker from Tencent Security Response Center found and reported the issue to XStream and provided the required information to reproduce it. ### For more information If you have any questions or comments about this advisory: * Open an issue in [XStream](https://github.com/x-stream/xstream/issues) * Email us at [XStream Google Group](https://groups.google.com/group/xstream-user)	2021-05-28	not yet calculated	CVE-2021-29505 CONFIRM
xwiki -- xwiki	### Impact A user without Script or Programming right is able to execute script requiring privileges by editing gadget titles in the dashboard. ### Patches The issue has been patched in XWiki 12.6.7, 12.10.3 and 13.0RC1. ### Workarounds There's no easy workaround for this issue, it is recommended to upgrade XWiki. ### References https://jira.xwiki.org/browse/XWIKI-17794 ### For more information If you have any questions or comments about this advisory: * Open an issue in [JIRA](https://jira.xwiki.org) * Email us at [XWiki security mailing-list](mailto:security@xwiki.org)	2021-05-28	not yet calculated	CVE-2021-32621 CONFIRM
xwiki -- xwiki	### Impact A user disabled on a wiki using email verification for registration can re-activate himself by using the activation link provided for his registration. ### Patches The problem has been patched in the following versions of XWiki: 11.10.13, 12.6.7, 12.10.2, 13.0. ### Workarounds It's possible to workaround the issue by resetting the `validkey` property of the disabled XWiki users. This can be done by editing the user profile with object editor. ### References https://jira.xwiki.org/browse/XWIKI-17942 ### For more information If you have any questions or comments about this advisory: * Open an issue in [Jira](http://jira.xwiki.org) * Email us at [Security mailing-list](mailto:security@xwiki.org)	2021-05-28	not yet calculated	CVE-2021-32620 MISC CONFIRM
yzmcms -- yzmcms	An issue was discovered in YzmCMS 5.8. There is a SSRF vulnerability in the background collection management that allows arbitrary file read.	2021-06-03	not yet calculated	CVE-2020-35970 CONFIRM
yzmcms -- yzmcms	A storage XSS vulnerability is found in YzmCMS v5.8, which can be used by attackers to inject JS code and attack malicious XSS on the /admin/system_manage/user_config_edit.html page.	2021-06-03	not yet calculated	CVE-2020-35971 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
yzmcms -- yzmcms	An issue was discovered in YzmCMS V5.8. There is a CSRF vulnerability that can add member user accounts via member/member/add.html.	2021-06-03	not yet calculated	CVE-2020-35972 CONFIRM
zzcmz2020 -- zzcms2020	An issue was discovered in zzcms2020. There is a XSS vulnerability that can insert and execute JS code arbitrarily via /user/manage.php.	2021-06-03	not yet calculated	CVE-2020-35973 MISC

Back to top

Subscribe to updates from Cybersecurity and Infrastructure Security Agency

Email Address e.g. name@example.com

Subscribe

Share Bulletin